Cyber-operaties en militair vermogen

Nederland lijkt in toenemende mate het slachtoffer te zijn van cyber-aanvallen. Dat wil zeggen: van cyber-criminaliteit, -spionage en -(h)ac(k)tivisme. Deze 'aanvallen' op DigiD, ING of iDeal waren niet de dreigingen die de minister van Defensie in juni 2012 voor ogen had toen hij de Defensie Cyber Strategie (DCS) lanceerde. Hierin was de ontwikkeling van militair vermogen om cyber-operaties uit te voeren een speerpunt. Tot nu toe is wereldwijd slechts mondjesmaat gebruik gemaakt van cyber-operaties tijdens militaire operaties.[1] Vaak verwijst men hierbij naar *Stuxnet*,[2] maar dit betreft 'cyber-sabotage' oftewel 'cybotage'.[3] Bij de Israëlische operatie *Orchard* zijn cyber-capaciteiten echter wel daadwerkelijk ingezet.[4] Het debat over de vraag hoe de Nederlandse krijgsmacht met dit 'nieuwe' domein zal omgaan is in volle gang.

*Kolonel dr. P.A.L. Ducheine en mr. J. van Haaster, tweede luitenant**

De uitdaging voor Nederland en Defensie is hoe *cyber warfare* in het militaire en veiligheidsdomein moet worden geïncorporeerd. Niet alleen bestaat er discussie of en in welke mate de overheid *cyber security* (meer) tot haar taken moet rekenen,[5] maar ook *hoe* de regering daartoe wordt uitgerust (door de wetgever).

Doel artikel

De vraag 'hoe organiseert de overheid digitale veiligheid (*cyber security*)?' keert ook terug binnen de verantwoordelijkheid van de Commandant der Strijdkrachten (CDS). Een aantal taken in het digitale domein wordt immers bij hem belegd.[6] Het onder de CDS ressorterende Defensie Cyber Commando zal uiteindelijk *cyber*-capaciteiten om moeten zetten in *operationele* capaciteiten die in normale militaire operaties te integreren zijn.[7]

Bij de lancering van de DCS zei de minister van Defensie hierover: 'Ons uitgangspunt is dat de cyber-capaciteiten van Defensie volledig geïntegreerd moeten worden in ons militair optreden'.[8] Met andere woorden, de CDS zal met cyber-capaciteiten bijdragen aan het militaire vermogen van Nederland.

* Kol Ducheine is universitair hoofddocent Cyber Operations aan de NLDA. Tlnt Van Haaster sloot zijn bachelor krijgswetenschappen af met een thesis over *Social Media* (bekroond door VID). De auteurs danken bgen b.d. prof. Hans Bosch, kolonel ir. Hans Folmer, de luitenant-kolonels Edwin de Ronde, mr. drs. Peter Pijpers en Marco Verhagen EMSD en majoor drs. George Dimitriu voor hun suggesties en commentaar.

1 P. Ducheine, F. Osinga & J. Soeters, *Cyber Warfare – Critical Perspectives* (Den Haag, TMC Asser Press, 2012).

2 Stuxnet is software die is aangetroffen in onderdelen van het Iraanse nucleaire programma en die onder meer centrifuges voor de verrijking van uranium ontregelde.

3 Een samentrekking van cyber en sabotage: Albert Benschop, *Cyberoorlog - Slagveld Internet* (Tilburg, Uitgeverij de Wereld, 2013).

4 Zie verder: P. Cornish, D. Livingstone, D. Clemente & C. Yorke, *On Cyber Warfare* (London, Chatham House, 2010).

5 R. Prins, 'Een cyberleger vergt geld en lef', *de Volkskrant*, 4 augustus 2012.

6 Defensie Cyber Strategie 2012 (hierna: DCS). Het Defensie Cyber Commando wordt via single service management bij het Commando Landstrijdkrachten ondergebracht.

7 A. Schnitger & J. Folmer, 'Cyber ontwikkelingen bij Defensie', in: *Intercom* (2012) (4) 17-19. Zie ook DCS.

8 Lezing minister van Defensie Defensie Cyber Symposium 2012 (Breda, 25-6-2012), via: <www.defensie.nl/actueel/nieuws/2012/06/27/46197032/Minister_Hillen_presenteert_Defensie_Cyber_Strategie>.

Hoe de krijgsmacht (en de CDS) cybercapaciteiten operationaliseert en integreert in het militaire vermogen, is een actuele vraag die ook in de *Militaire Spectator* aandacht krijgt.[9] Ons doel is bij te dragen aan de conceptuele vraag welke plaats cyber-operaties innemen binnen 'militair vermogen' en hoe de krijgsmacht *cyber warfare* kan operationaliseren.

In het bijzonder stellen we ons de vraag waartegen cyber-operaties zich richten (adressaat of aangrijpingspunt) en welke effecten met cyber-middelen kunnen worden bereikt.

Opzet

We zullen in deze bijdrage de conceptuele en doctrinaire vragen binnen het militaire machtsinstrument aan de orde stellen. Daarbij concentreren we ons op de eerste en de tweede hoofdtaak: verdediging, en handhaving en bevordering van de internationale rechtsorde. Om niet alleen maar ingewijden in de militaire doctrine te bereiken bezien we eerst de essentiële aspecten van de gangbare conceptuele en doctrinaire benadering van reguliere militaire operaties.[10] Daarna bespreken we 'militair vermogen' en haar context, alsmede de inzet van militair vermogen, oftewel operaties. We staan stil bij de vraag welke effecten met operaties worden beoogd, welke middelen en methoden daarvoor bestaan en waartegen ze zich richten.

Onze hoofdinspanning betreft de introductie van het digitale domein in het militair vermogen. We beschrijven de bijzondere en gelaagde structuur van *cyberspace* en bepalen de cyber-elementen binnen de drie componenten van militair vermogen.

Vervolgens definiëren en beschrijven we cyber-operaties, en kijken we waar deze operaties zich op richten, welke effecten mogelijk zijn en welke middelen en methoden daarbij gebruikt zouden kunnen worden.

Uitgangspunten, definitie & beperkingen

Om een eenduidige begripsvorming te realiseren baseren we ons allereerst op gangbare begrippen uit de militaire doctrine.[11] We beschrijven de generieke doctrine overigens slechts op hoofdlijnen. Daarnaast hanteren we een internationaal gangbare definitie voor militaire cyber-operaties:[12]

> *The employment of cyber capabilities with the primary purpose of achieving [military] objectives in or by the use of cyberspace.*[13]

Het uitvoeren van cyber-operaties hebben we hiervoor aangeduid als *cyber warfare*.[14] Wat *cyber capabilities* zijn, welke doelstellingen te realiseren zijn en waaruit cyberspace bestaat, zullen we later in meer detail uiteenzetten.[15]

Van militair vermogen naar operaties

Veiligheid garanderen is een van de kerntaken van de staat. Voor de realisatie van veiligheidsbeleid en (andere) strategische doelen beschikken staten over meerdere machtsmiddelen: diplomatieke, economische, militaire en informatie.[16] Het doel van de inzet van deze machtsmiddelen is het beïnvloeden van (het gedrag van) andere actoren waardoor veiligheidsbeleid en strategische doelen te realiseren zijn. 'De Nederlandse defensieinspanning is gericht op het nationaal belang, de bescherming en bevordering van de Nederlandse waarden en buitenlandpolitieke doelstellingen', aldus de NDD.[17]

9 De *Militaire Spectator* bood tot nu toe plaats aan vier artikelen inzake *cyber warfare* en *cyber security*. Recent uitte de redactie zich via een Editoriaal over het belang van 'soft cyber' (het gebruik van sociale media e.d.): 'Cyber en militair vermogen', *Militaire Spectator* 181 (2012) (12) 530-531. Zie ook Graaf en Tettero (2010); Ducheine & Voetelink (2011-6); Akerboom (2012-12); en H-J van der Molen 'Cybersecurity - Relevante trends voor Defensie' (2013-03).

10 Doctrinair ingewijden kunnen deze uiteenzetting van het 'militaire denken' overslaan en volstaan met het bestuderen van figuur 2-4.

11 We baseren ons op de (in druk zijnde) nieuwe Nederlandse Defensie Doctrine (Concept d.d. maart 2013).

12 'Digitaal' en 'cyber' zullen we als synoniemen hanteren.

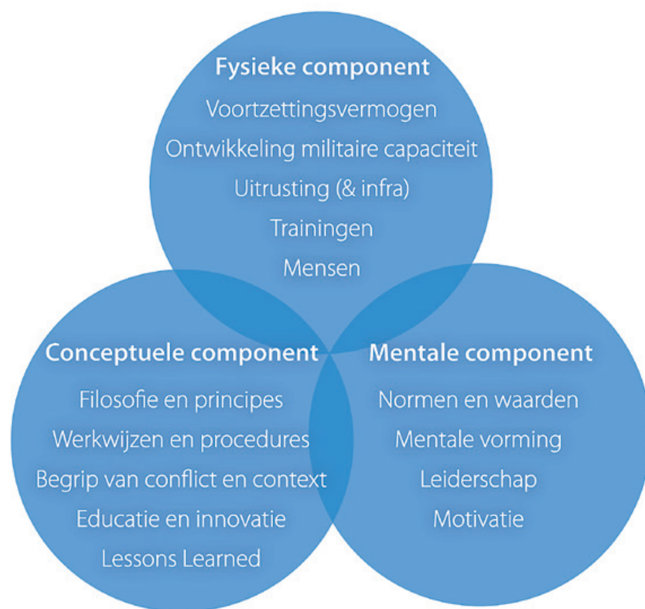
13 M.N. Schmitt (ed.). *Tallinn manual on the international law applicable to cyber warfare* (New York, Cambridge University Press, 2013) 258.

14 Waarbij we *warfare* (oorlogvoering) als fenomeen gebruiken. Voor een specifieke en beperkte betekenis: P.A.L. Ducheine, 'Legal Framework for Military Cyber Operations', in *Militair Rechtelijk Tijdschrift* 106 (2013) (1) 9-19.

15 Let wel: capaciteiten zijn middelen, *capabilities* is vermogen.

16 Ministerie van Defensie, *Nederlandse Defensie Doctrine* (2013) 21. Hierna: NDD (2013). Zie t.a.p. de alternatieve indelingen van machtsmiddelen/-instrumenten.

17 NDD (2013) 48.



Figuur 1. Militair vermogen

Het militaire machtsmiddel – de krijgsmacht dus – kan gedrag van andere statelijke en niet-statelijke actoren beïnvloeden via afschrikking, dwang en – ultimo – interventie met gebruik van geweld,[18] maar óók door samenwerking, training of (logistieke) steun.

Militair vermogen

De krijgsmacht genereert en levert militair vermogen (*fighting power*), omschreven als 'de totale capaciteit die de krijgsmacht levert om strategische functies te vervullen'.[19] Militair vermogen bestaat uit drie componenten: de fysieke, de conceptuele en de mentale (zie figuur 1).[20]

De fysieke component – gevechtskracht of *combat power* – bestaat allereerst uit 'personeel en materieel dat georganiseerd wordt ingezet in een operatie'.[21] Bij materieel moeten we denken aan goederen, infrastructuur, voer-, vaar- en vliegtuigen en uitrusting. Daarnaast behelst de fysieke component voortzettingsvermogen (*sustainability*) en operationele gereedheid (*readiness*).[22]

De mentale component bestaat uit factoren die onderling samenhangen: motivatie, leiderschap, mentale vorming, normen en waarden en tot slot 'perceptie van de toestand'.
Ter completering: doctrine, militair denken en principes, opleidings- en trainingsfilosofie vormen samen de conceptuele component.

De CDS beschrijft de synergie van de drie componenten van militair vermogen: 'Militair vermogen omvat meer dan uitsluitend de beschikbaarheid van operationele middelen (capacities). Men moet ook bereid en in staat (*capable*) zijn om deze middelen in te zetten. Als dit goed ontwikkeld is, dan spreekt men van militair vermogen (en worden *capacities* verheven tot *capabilities*)'.[23]

Militair vermogen wordt dus vanuit een strategische doelstelling, al dan niet samen met andere instrumenten van macht, aangewend om het gedrag van actoren te beïnvloeden.[24]

Aanwenden van militair vermogen

Militair vermogen wordt concreet doordat de krijgsmacht daadwerkelijke activiteiten, operaties genoemd, uitvoert. Operaties zijn divers in vorm, doelstelling, omvang en duur. Ze spelen zich af in verschillende domeinen: land, zee, lucht, (ruimte) en in het informatie- en digitale domein (zie hierna).

Schematische weergaven van het aanwenden van militair vermogen, oftewel een conceptueel model van operaties, kennen we bijvoorbeeld uit de *Land Doctrine Publicatie* II-C voor het optreden tegen irregulier optredende tegen-

18 NDD (2013) 22 en 41. In het Rapport Verkenningen wordt dit op een vergelijkbare wijze omschreven via (het gebruik van) strategische functies, bijvoorbeeld anticiperen, voorkomen, afschrikken, beschermen, interveniëren, stabiliseren, normaliseren. Ministerie van Defensie, *Eindrapport Verkenningen- Houvast voor de krijgsmacht van de toekomst* (2010)193.

19 NDD (2013) 71. Of zoals in NDD (2005) 50: 'de capaciteit om militaire operaties uit te voeren'.

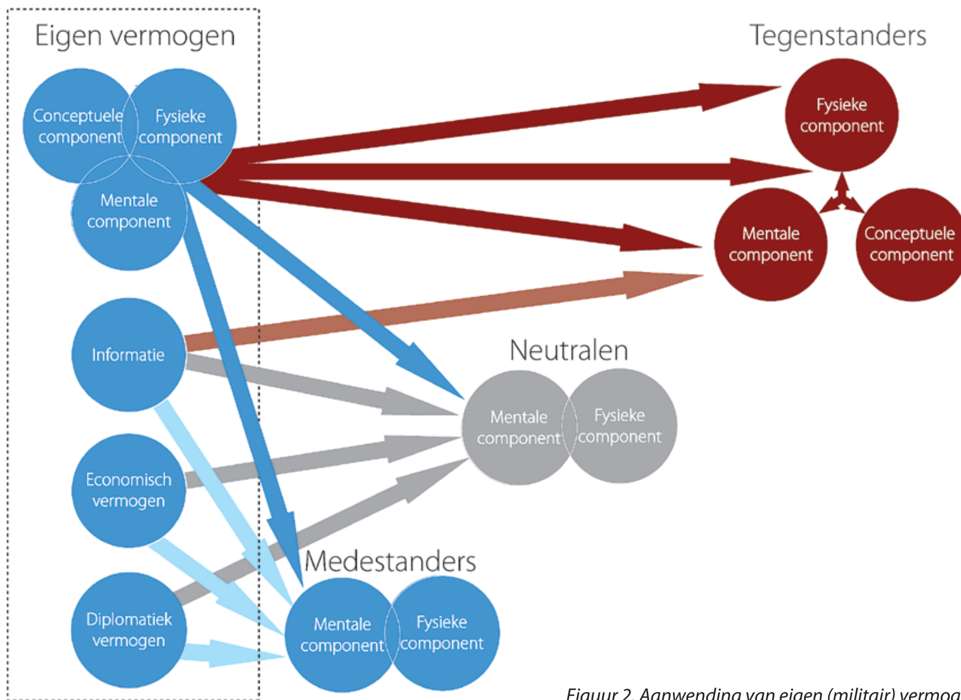
20 Naar de onderverdeling in: Koninklijke Landmacht, *DP 3.2 Landoperaties*, (concept versie 2.2, december 2012) 1-8. De onderverdeling verschilt per doctrinepublicaties: zie NDD (2013) 74, LDP-1 106, en DP 3.2 Landoperaties.

21 NDD (2013)77.

22 NDD (2005). Idem *DP 3.2 Landoperaties* 1-8/9.

23 NDD (2013)74, § 4.2.

24 Indien de instrumenten van macht in samenhang en gecoördineerd worden ingezet, mogelijk zelfs in internationaal verband, spreken we van een geïntegreerde benadering of *comprehensive approach*.



Figuur 2. Aanwending van eigen (militair) vermogen

standers.[25] We gebruiken dit model hier in een aangepaste vorm, die aansluit bij de manoeuvrebenadering en bij de geïntegreerde benadering.

De eerste aanpassing houdt in dat we naast tegenstanders ook medestanders en neutrale actoren toevoegen. Het beïnvloeden van actoren is een centrale notie. In de manoeuvrebenadering (*manoeuvrist approach*) wordt het eigen militaire vermogen vooral ingezet tegen onderkende zwakheden van andere actoren.[26] Operaties richten zich daarbij niet zozeer op de fysieke maar op de mentale component, en de samenhang tussen de drie componenten van het (militair) vermogen van anderen.[27] De nieuwe NDD verwoordt dit als volgt:

> *Effectief optreden wordt bepaald door benadering van alle actoren en niet alleen door de wijze waarop een tegenstander wordt benaderd. In het verlengde hiervan kan daarom de 'wil van de vijand' uit de traditionele manoeuvrebenadering worden gezien als de 'opinie van de actor'. De opinie vertaalt zich in steun en daarmee in samenhang ('cohesion').*
>
> *Steun voor het eigen optreden moet worden behouden en vergroot. Steun voor de tegenstander moet worden beperkt, zodat hij uiteindelijk opgeeft. Door de eigen activiteiten gewogen af te stemmen op de 'will', 'understanding' en 'cohesion' van alle actoren, wordt invulling gegeven aan het denken in effecten en de manoeuvrebenadering in bredere zin.*[28]

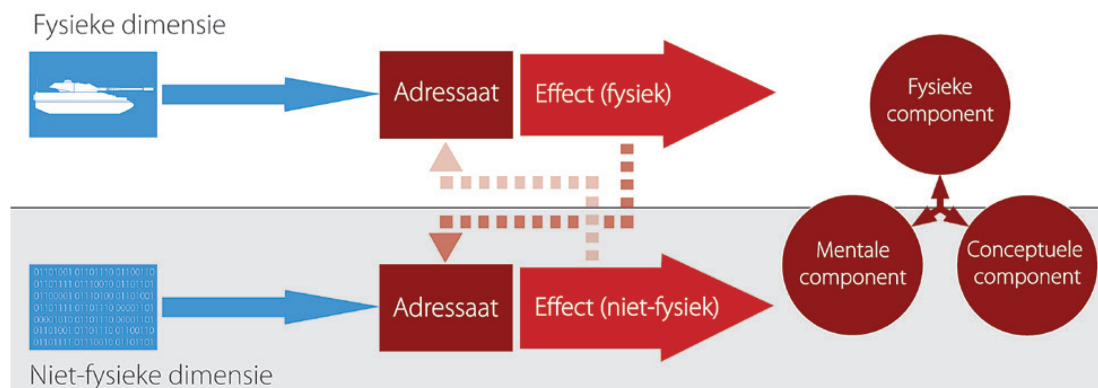
Figuur 2 visualiseert hoe het vermogen van tegenstanders, neutralen én medestanders wordt beïnvloed. Het belang van (aanvankelijk) neutrale partijen mag niet worden onderschat. Zo nam het aanvankelijk neutrale Anonymous onverwacht een zeer actieve rol aan in de Tweede Gazaoorlog en werd één van Israëls tegenstanders.

25 Koninklijke Landmacht, *Landmachtdoctrinepublicatie II-C: Gevechtsoperaties, gevechtsoperaties tegen een irregulier optredende tegenstander* (LDP II Deel C) (Zwolle, PlantijnCasparie, 2003) 529.

26 NDD (2013)120: 'Deze benadering is gericht op het beïnvloeden van de perceptie van de werkelijkheid, het gedrag en het optreden van actoren. Belangrijke aspecten hierbij zijn momentum, tempo en mentale beweeglijkheid (*agility*) die gecombineerd leiden tot een schokeffect en verrassing bij de actoren'.

27 NDD (2013)120-121.

28 NDD (2013)122.



Figuur 3. Middel-adressaat-effect

De inzet van machtsmiddelen zal er op gericht zijn dat deze neutrale partijen in ieder geval geen tegenstander worden: bij voorkeur medestander, maar minimaal neutralen.

Concreet betekent dit dat via operaties onder meer wordt getracht de samenhang tussen de componenten van het vijandelijke militaire vermogen te verbreken. Dit verbindende element is kwetsbaar en kan slechts in stand blijven bij de gratie van onder meer (de toegang tot) goede informatie.

Vervolgens wordt getracht de vijandelijke mentale component te degraderen en ten slotte (indien nodig) de vijandelijke fysieke component te reduceren. Vermogens van medestanders kunnen via de fysieke én de mentale lijn worden versterkt.

De tweede aanpassing van het model behelst het toevoegen van andere machtsinstrumenten, zoals diplomatiek vermogen en informatie, naast het militaire vermogen om actoren – tegenstanders, medestanders en neutralen[29] – via de geïntegreerde benadering te beïnvloeden.[30]

Het ‘beïnvloeden’ van tegenstanders met militaire middelen is vaak disruptief; we gebruiken ook wel de term ‘aangrijpen’. Bij medestanders en neutralen is die beïnvloeding doorgaans constructief van aard.

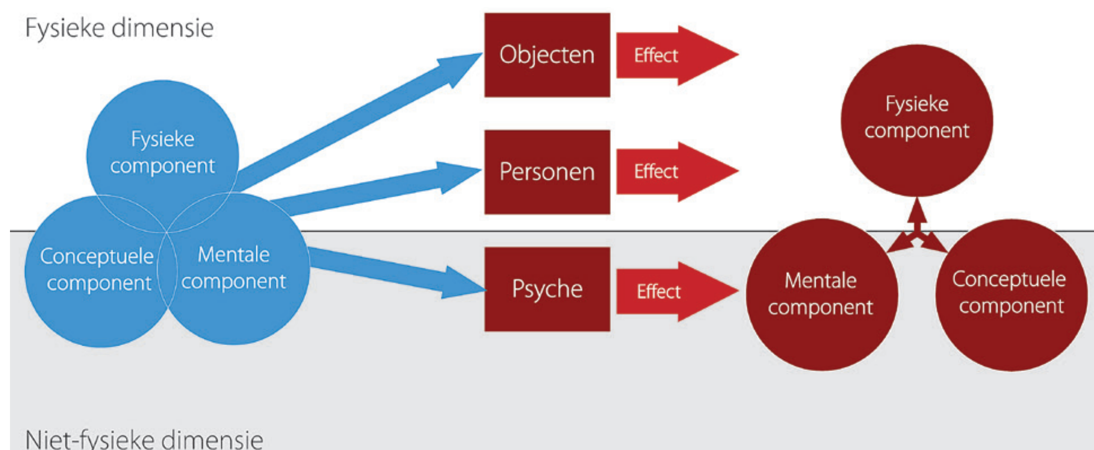
Effecten en middelen

De daadwerkelijke activiteiten van de krijgsmacht leveren effecten op. In de aanwending van militair vermogen staan de manoeuvrebenadering en het denken in effecten, hun onderlinge relatie, hun relatie met actoren en de operationele omgeving centraal.[31]

De (beoogde) effecten zijn al dan niet fysiek van aard.[32] De daadwerkelijke vernietiging van een vijandelijk eskadron ligt in het fysieke vlak; ‘breken’ van de wil van deze eenheid ligt echter in het niet-fysieke, psychologische vlak. Fysieke effecten en psychologische effecten hebben meestal een wisselwerking op elkaar: zo kan de dood van een collega de wil breken van diens *buddy*.

De beoogde effecten worden met fysieke (harde) middelen, *hard power*, en niet-fysieke (zachte) middelen, *soft power*, gerealiseerd (zie figuur 3).[33] Een tank is een voorbeeld van een fysiek middel; informatie verstrekken of ‘steun’ is een voorbeeld van een niet-fysiek middel.

29 Zodat deze zich hetzij afzijdig dan wel als medestander op zullen (blijven) stellen.
30 *Comprehensive approach*: NDD (2013)29: ‘Bij een geïntegreerde benadering worden de machtsmiddelen die een staat ten dienste staan, op gecoördineerde en samenhangende wijze ingezet, bij voorkeur in een coalitie met andere landen en in een samenwerkingsverband met internationale en niet-gouvernementele organisaties’.
31 *DP 3.2 Landoperaties*, 6-21.
32 NDD (2013) 117: ‘Effecten kunnen zowel in het fysieke als het psychologische vlak worden bereikt’. Voor zover de effecten fysiek van aard zijn, betreft het zowel lethale als niet-letale effecten.
33 *DP 3.2 Landoperaties*, 4-6: ‘Niet alleen de inzet van wapengeweld sorteert deze effecten. Beïnvloeding van tegenstanders door hun informatie en informatie-infrastructuur, hun financiële bronnen en hun draagvlak aan te tasten, is een bredere toepassing’.



Figuur 4. Middelen, adressaat en effecten

Het specifieke adressaat van militaire operaties, van middelen en methoden speelt een rol in het navolgende deel.

Adressaat

De vraag is tegen welke elementen van het (militaire) vermogen van andere actoren – tegenstanders, medestanders en neutralen – militaire operaties zich precies richten; wat is het aangrijpingspunt? We hanteren hiervoor zoals gezegd de term 'adressaat'.[34] Oftewel: waartegen worden fysieke en niet-fysieke middelen (hard en soft power) ingezet om effecten in het fysieke en/of het psychologische vlak te realiseren? De fysieke component kan worden aangegrepen via mensen en objecten (zie figuur 4).

'Mensen' betreft zowel individuen als groepen die deel uitmaken van (potentiële) tegenstanders, neutralen en medestanders (inclusief de eigen troepen en bevolking). Bij 'objecten' gaat het om fysiek tastbare goederen zoals uitrusting, materieel, logistieke voorraden en infrastructuur (zie ook figuur 1).

Het beïnvloeden van de mentale component geschiedt via de 'psyche', oftewel door het beïnvloeden van motivatie, wil, gevechtsbereidheid en de effectiviteit van leiderschap via het overbrengen van informatie, signalen, indrukken, et cetera. Daarnaast wordt de perceptie van de situatie of het begrip van de toestand beïnvloed. Die effecten zijn niet-fysiek.

De samenhang tussen de drie componenten van (militair) vermogen kan worden aangegrepen door cruciale onderdelen van leiderschap, besluitvorming en bevelvoering, commandovoeringsondersteuning en informatieverwerking (objecten, informatie en processen) uit te schakelen of te beïnvloeden. Uiteindelijk valt dit ook terug te voeren op generieke adressaten: mensen, objecten en psyche.

Een belangrijk gegeven is de wisselwerking tussen fysieke en niet-fysieke aangrijpingspunten en effecten (zie terug).

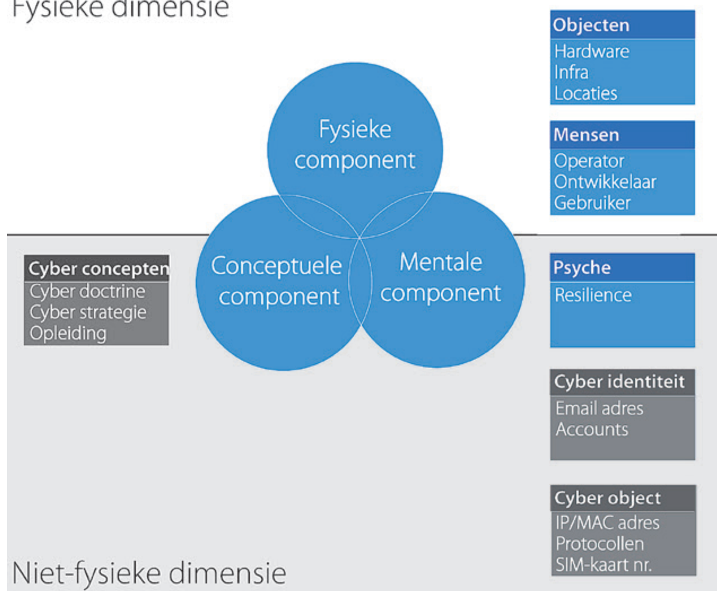
Effecten

Effecten worden in verschillende dimensies (fysiek en niet-fysiek) via militaire operaties – solitair of geïntegreerd, *joint* en/of *combined* – gerealiseerd.[35]
De fysiek bepaalde domeinen land, zee, lucht (en ruimte) zijn qua middelen te koppelen aan de fysieke dimensie, terwijl de gewenste effecten zowel in het fysieke als in het niet-fysieke vlak kunnen liggen.

We zullen deze doctrinaire inzichten hierna aanvullen met het digitale domein en digitale

34 Om verwarring met de LDP-1 (99) te voorkomen, gebruiken we hierna alleen de term 'adressaat'.

35 *Joint*: verschillende krijgsmachtdelen werken samen; *combined*: krijgsmachten van verschillende staten werken samen.



Figuur 5. Cyber capabilities en militair vermogen

operaties.[36] We besteden daarbij aandacht aan cyber-operaties en hun beoogde effecten, beschikbare middelen en methoden en het adressaat.

Het digitale domein

De eerste vraag is uiteraard: wat is het digitale domein of cyberspace? Het digitale domein onderscheidt zich van de andere domeinen doordat het niet geografisch of fysiek afgebakend is. Dit betekent overigens niet dat het digitale domein of cyberspace geen fysieke elementen bevat. Integendeel. Het digitale domein wordt gedefinieerd als 'het geheel van ICT-middelen en ICT–diensten'.[37] Dit domein bestaat ook uit 'alle niet met internet verbonden netwerken of andere digitale apparaten'.[38]
Los van deze definitie is het natuurlijk de eerste vraag hoe cyberspace er uitziet.

Het digitale domein heeft een aantal 'lagen' of onderdelen. Voor het doel van deze bijdrage volstaat een tweedeling: een fysieke en een niet-fysieke laag.[39] De fysieke laag bestaat uit geografische locaties en fysieke objecten zoals hardware (computers, *servers*, *routers*, *smartphones*) en hun fysieke verbindingen (zoals glasvezelkabels, zendmasten).[40] Tot de fysieke dimensie rekenen wij ook mensen: de gebruikers en bedienaars van de middelen en capaciteiten binnen dit domein.[41]

Het unieke van het digitale domein ligt in de tweede, de virtuele laag (*logical layer*), bestaande uit protocollen, software en digitale verbindingen tussen fysieke knooppunten en onderdelen in het netwerk.[42] Bovendien bevat deze laag de applicaties en software binnen de onderdelen van het netwerk zelf. Deze laag bevat eveneens data in de vorm van de cyber-identiteiten van mensen (e-mailadressen, digitale accounts op *Facebook*, *Linkedin*, gsm-telefoonnummers) en cyber-objecten (zoals IP-adressen, MAC-adressen en SIM-kaartnummers).[43]
Deze virtuele laag maakt het mogelijk dat de objecten en personen binnen een fysieke netwerkinfrastructuur met elkaar kunnen communiceren en dat data-overdracht mogelijk is.[44]

36 Cyberspace wordt (al dan niet terecht) het vijfde domein genoemd. Zie onder meer NATO (2010) AJP 01d, 5-14 en NDD (2013) 81.
37 Adviesraad Internationale Vraagstukken en Commissie van Advies inzake Volkenrechtelijke Vraagstukken (AIV & CAVV, 2011): *Digitale oorlogvoering*, Den Haag: AIV no. 77; CAVV no. 22, zie <www.aiv-advice.nl>, bijlage III.
38 AIV/CAVV (2011), bijlage III.
39 De niet-fysieke laag bestaat weer uit meerdere sub-lagen. Het OSI model hanteert zeven lagen: de fysieke laag, de datalink-laag, de netwerklaag, de transportlaag, de sessielaag, de presentatielaag en de applicatielaag. Het gelaagde OSI model wordt wereldwijd gebruikt als referentiemodel voor netwerkcommunicatie, zie: <www.tekstenuitleg.net/artikelen/netwerken/osi-model/osi-model.html>. TCP/IP hanteert vier lagen: applicatielaag, transportlaag, internetlaag, network interface, zie <technet.microsoft.com/nl-nl/library/cc786900(v=ws.10).aspx>. Drie lagen komen terug in: United States Army Training and Doctrine Command (TRADOC 2010), *The United States Army's Cyberspace Operations Concept Capability Plan 2016–2028*, TRADOC Pamphlet 525-7-8, <www.tradoc.army.mil/tpubs/pams/tp525-7-8.pdf>, 8. Zie ook L. Tabansky, 'Basic Concepts in Cyber Warfare', in: *Military and Strategic Affairs* 3 (2011)(1), 75-92, 78.
40 TRADOC (2010) 8.
41 In sommige indelingen maken personen (en hun cyber-identiteit) deel uit van een derde laag: de sociale laag. Zie bijvoorbeeld TRADOC (2010) 9.
42 TRADOC (2010) 9.
43 Internet Protocol (IP)-adressen, Media Access Control (MAC)-adressen, Subscriber Identity Module (SIM) -kaart.
44 Let wel: *DP3.2 Landoperaties* typeert het elektromagnetische spectrum als een fysiek fenomeen: 4-6, § 4213.

De niet-fysieke virtuele laag met de daarin besloten liggende capaciteiten en risico's maakt cyberspace bijzonder.

Het digitale domein en militair vermogen
De volgende vraag is welke cyber-elementen bijdragen aan militair vermogen. We analyseren dit voor de fysieke, de mentale en de conceptuele componenten (zie figuur 5). Daarbij doet zich een indelingsvraagstuk voor omdat een aantal niet-fysieke elementen van cyber-vermogen zich lastig laat onderbrengen in de klassieke driedeling.

Fysieke component
De fysieke laag van het cyber-domein rekenen we tot de fysieke component van militair vermogen: het gaat – net als in de normale wereld – op de eerste plaats om objecten en mensen. De objecten betreffen alle knooppunten in het netwerk (hardware zoals routers, servers en computers),[45] fysieke verbindingen (zoals glasvezel- of koperkabel) en objecten voor niet-kabelgebonden verbindingen (zendmasten e.d.) tussen de knooppunten.[46]

'Mensen' betreft allereerst operators, bedienaars van de objecten en daarnaast gebruikers in het digitale domein, bijvoorbeeld twitteraars en volgers, alsmede softwareontwikkelaars en hackers (in overheidsdienst).

Naar analogie van het reguliere fysieke vermogen noemen we ook cyber-oefeningen, oefenfaciliteiten en de ontwikkeling van cyber-capaciteit.[47] Daar hoort onder meer een 'oefenlaboratorium' bij: een veilige testomgeving om met digitale 'wapens' en methoden te oefenen.[48]

Virtuele afspiegeling van fysieke elementen
Mensen en objecten in het cyber-domein moeten kunnen communiceren, waarvoor gebruik wordt gemaakt van software, applicaties, accounts en protocollen uit de virtuele laag. Dat levert, zoals gezegd, een indelingsprobleem op, dat we nu zullen adresseren.

De virtuele afspiegeling van objecten en mensen rekenen we niet tot de fysieke component van



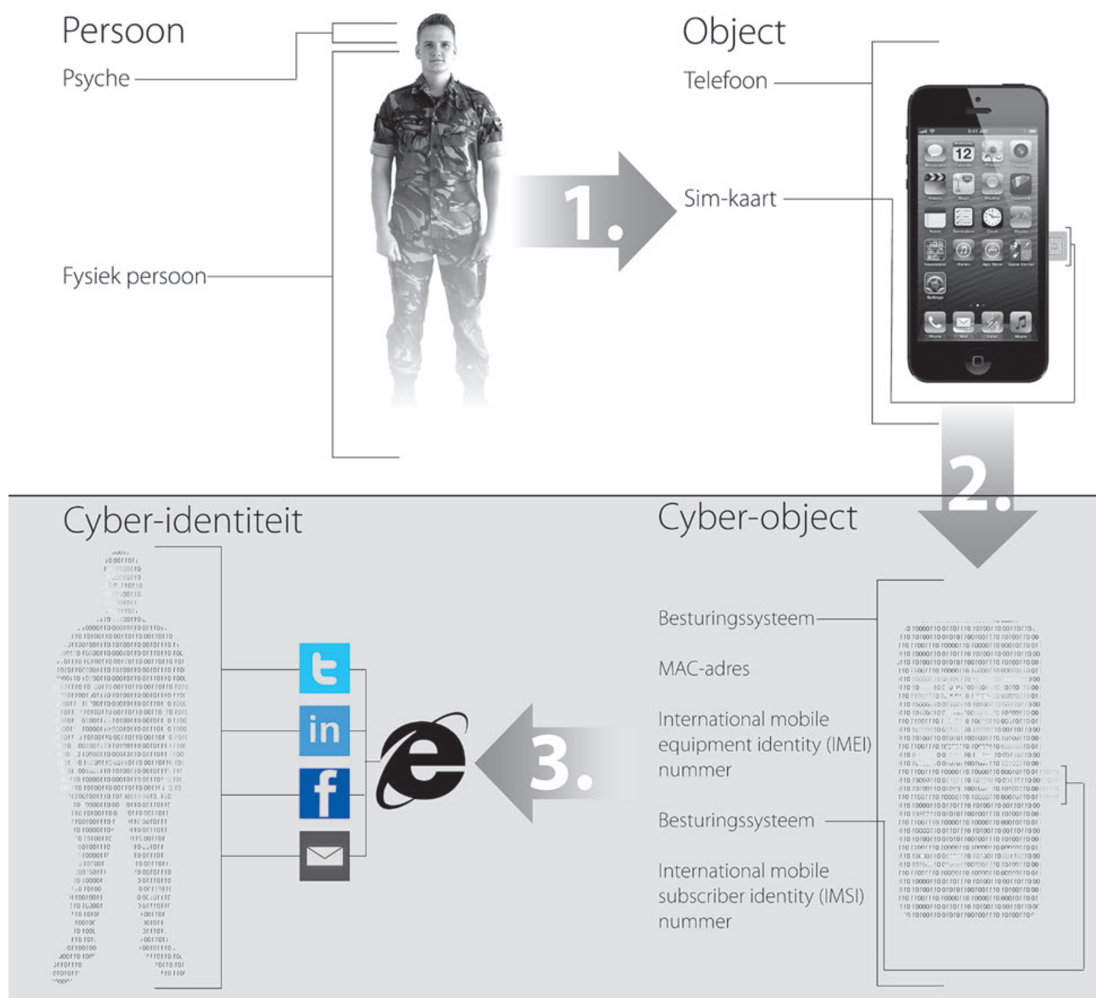
Figuur 6. De cyber-identiteit van Jeanine Hennis-Plasschaert (https://twitter.com/JeanineHennis/status/268006560788254722

militair vermogen. Ze zijn immers niet fysiek, niet tastbaar. Het gaat 'slechts' om een reflectie van fysieke onderdelen. Het zijn virtuele elementen die onlosmakelijk – maar niet één op één – te relateren zijn aan fysieke objecten en mensen. We noemen deze cyber-objecten en cyber-identiteiten.

Zoals gezegd faciliteert de virtuele laag van het digitale domein de fysieke laag zodat communicatie mogelijk is. De logical layer bestaat uit verschillende cyber-objecten: virtuele onderdelen zoals software, protocollen (bijvoorbeeld Internet Protocol of IP)[49], processen (e-mail, encryptie, *Domain Name System*), adressen (bijvoorbeeld IP- en MAC-adressen, SIM-kaart nummers)[50] en overige data (zoals besturingssystemen).[51]

Mensen én wat we hun psyche hebben genoemd (wat op zich al een virtueel aspect is)

45 TRADOC (2010), 9.
46 J. Andress & S. Winterfeld, Cyber Warfare: *Techniques, Tactics and Tools for Security Practitioners* (Waltham, Syngress, 2011) 120.
47 Bijvoorbeeld de oefening *Locked Shield* 2013, waarbij het Nederlandse team de derde plaats behaalde. Zie: http://www.ccdcoe.org/401.html .
48 Zie voor een omschrijving van basiswaarborgen voor fysieke netwerkinfrastructuur: C.P. Pfleeger & S.L. Pfleeger , *Security in Computing* (4th Ed.) Prentice Hall, 2007, 442-443.
49 Ook: OSI, IPv4/6, http, HTML, TCP, UDP.
50 IP-adres: een nummer voor een internetaansluiting voor hardware. MAC-adres: uniek nummer van hardware.
51 Pfleeger & Pfleeger (2007) 385-386.



Figuur 7. Relatie personen, objecten en cyber-objecten en cyber-identiteiten.

kennen ook een virtuele equivalent in het cyber-domein: de cyber-identiteit (of *cyber personality*). Steeds meer sociale en beroepsmatige aspecten van mensen spelen zich af in het cyber-domein,[52] zoals via sociale media.[53] Veel mensen hebben, om bereikbaar en verbonden te zijn, informatie online staan en beschikken over een of meerdere *cyber-identiteiten*. Cyber-identiteiten bestaan uit profielgegevens op sociale media, mailadressen, blogs en alle andere data die online staan en gelieerd zijn aan een bepaald persoon (zie figuur 6). Twitter- en Facebook-accounts zoals *@Landmacht* of <*www.facebook.com/Commandantderstrijdkrachten*> zijn sprekende voorbeelden.[54]

Overigens kan één persoon meerdere identiteiten hebben, één identiteit kan meerdere personen betreffen en sommige identiteiten representeren niet wat ze suggereren: *@Koning_NL*, *@MinisterHennis* en

52 C.L. Coyle & H. Vaughn, 'Social networking: Communication revolution or evolution?', in: *Bell Labs Technical Journal* 13 (2008)(2)13-17; S. Matthews, 'On-line Professionals', in: *Ethics and Information Technology* 8 (2006) 66; M. Miller & D. Slater, *The Internet: An Ethnographic Approach* (Oxford, Berg. Chapter One – Conclusions, 2006); Antoci et al., *See you on Facebook: the effect of social networking on human interaction*, (European Research Institute on Cooperative and Social Enterprises, 2010) 182.

53 Antoci (2010); PCCLM (2011), *A Survey on What Content do People Share Online and With Whom?* <pcclm.com/2011/05/survey-on-what-do-people-share-content.html>.

54 Zie 'Cyber en Militair Vermogen', in: *Militaire Spectator* 181 (2012)(12) 530-531.

Toelichting figuur 7
In de fysieke laag treffen we een persoon en een fysiek object met internetverbinding, bijvoorbeeld een smartphone, waarmee hij toegang heeft tot de cyberspace (stap 1).[a] *De telefoon bestaat uit twee relevante fysieke onderdelen: een SIM-kaart*[b] *en het toestel zelf. Deze fysieke objecten hebben een digitale representatie in de virtuele laag via drie cyber-objecten (stap 2). Allereerst het International Mobile Equipment Identity (IMEI)-nummer dat gekoppeld is aan het toestel. Daarnaast heeft het toestel een MAC-adres dat gebruikt worden om het toestel binnen een netwerk te identificeren en dataoverdracht te faciliteren. Op de derde plaats het International Mobile Subscriber Identification (IMSI)-nummer dat de gebruiker als abonnee identificeert.*[c] *Het ISMI- nummer is opgeslagen op de SIM-kaart die de gebruiker bij het afsluiten van een vast abonnement of bij aanschaf van een 'beltegoed' variant in bezit krijgt.*[d]
De fysieke objecten (smartphone en SIM-kaart) én de cyber-objecten (IMEI-, IMSI-nummer en MAC-adres) faciliteren de gebruiker en diens virtuele manifestaties: de cyber-identiteiten (stap 3). Via zijn IMSI-nummer kan hij gebruik maken van internet en zijn cyber-identiteiten opbouwen via online services zoals Twitter en e-mail.

a Vanwege de overzichtelijkheid hanteren we slechts de mannelijk aanduiding of verwijzingsvorm: hij/zijn.
b *Subscriber Identity Module* (SIM) is een smartcard waarop de gegevens staan van een aansluiting/abonnee van een mobiele telefoon.
c *MSI identificeert een gebruiker via een SIM-kaart of IMEI-nummer.* Zie www.princeton.edu/~achaney/tmve/wiki100k/docs/International_Mobile_Subscriber_Identity.html.
d IMEI identificeert een toestel..

<*www.facebook.com/gentom.middendorp*> zijn 'nep' accounts.[55]
In figuur 7 hebben we de relatie tussen de fysieke en de virtuele dimensie uiteengezet en demonstreren we hoe de virtuele representatie van fysieke elementen werkt in het geval van een smartphone.

Conceptuele en mentale component
Net als andere operaties zullen ook cyber-operaties doctrinair worden voorbereid en uitgevoerd. De doelstelling van onze bijdrage sluit daarbij aan: doctrine, grondbeginselen en principes, lessen, opleidings- en trainingsfilosofie op het concept cyber warfare en zijn implicaties moeten worden doorgrond. Uiteraard moet dit vervolgens in opleidingen worden geïncorporeerd. Via eerder genoemde trainingen en oefeningen (zie de fysieke component) draagt dit bij aan het militaire vermogen als geheel. Het personeel dient ook gemotiveerd te zijn en over een militaire *mindset* te beschikken waardoor het in staat is en blijft de cyber-doctrine uit te voeren.[56] Deze aspecten vinden we terug in de conceptuele en de mentale component.

De samenhang tussen de drie componenten alsmede de integratie van cyber-operaties en -capaciteiten in andere onderdelen van militair vermogen, in operaties én in andere machtsinstrumenten, moet eveneens worden doordacht. Militaire planners moeten bekend zijn met de samenhang tussen de verschillende lagen van cyberspace. Dat heeft, met andere woorden, invloed op de conceptuele en mentale component. Ook de interactie tussen sociale, technische en operationele (militaire) processen moet kunnen worden begrepen en gehanteerd. Met cyber warfare zet de krijgsmacht andermaal stappen in de niet-kinetische dimensie, een ontwikkeling die herkenbaar is uit recente COIN-ervaringen.

Wat nu reeds opvalt is het feit dat het digitale domein een niet-fysieke laag met virtuele capaciteiten heeft: cyber-objecten en cyber-identiteiten. Is dit volstrekt nieuw? Enerzijds niet als we het 'denken in effecten' en de inzet van 'soft power' in ogenschouw nemen. In dat opzicht vormen deze virtuele (cyber-) capaciteiten slechts een uitbreiding. Anderzijds is hiermee sprake van volstrekt nieuwe elementen, dito capaciteiten en mogelijkheden, maar ook nieuwe risico's.

55 Idem: @*WillemAlexander*, zie <twitter.com/WillemAlexander>.
56 Een militaire *mindset*: zie A. Benschop, *Cyberoorlog* (Tilburg, Uitgeverij de Wereld, 2013). Voor een omschrijving van de '*cyber warrior*': Andress & Winterfeld (2011)61-69.

Zelfs al zou dit geen doctrinaire gevolgen hebben, het enkele feit dat cyber-identiteiten en cyber-objecten bestaan, is relevant voor doctrinair denken. Deze extra mogelijkheden (en kwetsbaarheden) vragen om bewustwording, acceptatie en adaptatie van de virtuele dimensie en de samenhang met de fysieke. Cyber warfare is meer dan 'het aanvallen van een hacker' of het 'targeten van een server', zoals regelmatig wordt gehoord.

Een ander markant feit is de relatie tussen cyber-operaties en informatieoperaties.[57] We volstaan hier met de opmerking dat cyber-operaties qua principe informatieoperaties volgen, maar qua adressaat een unieke positie innemen. Ook 'soft cyber'-operaties zijn daardoor afwijkend ten opzicht van gangbare informatieoperaties.

Een laatste factor van invloed is de rol en betekenis van geografie en ruimte in cyberspace. Deze is anders dan bij louter kinetische operaties. Actoren (en fysieke objecten die deel uitmaken van het cyber-domein) kunnen zich overal ter wereld bevinden. Dit wil niet zeggen dat cyber warfare ontdaan is van fysieke grenzen. Sterker nog, deze spelen nog steeds een belangrijke rol: objecten en mensen bevinden zich namelijk in de fysieke laag. Maar met internet als vector en het gebruik van cyber-objecten en cyber-identiteiten, zijn afstanden erg kort, en de 'ruimte' waarin operaties plaatsvinden ('het slagveld') erg groot. Hoewel de virtuele elementen tot fysieke onderdelen zijn te herleiden, kan de geografische locatie daarvan weer complicaties opleveren indien cyber-operaties worden overwogen.[58]

Cyber in militair vermogen

Doordachte integratie van cyber-capaciteiten in andere onderdelen van militair vermogen, in operaties én in andere machtsinstrumenten, is een vereiste. Cyber capabilities vinden we in de vertrouwde fysieke, conceptuele en mentale component van (militair) vermogen, namelijk personen (inclusief groepen en militaire eenheden), objecten (inclusief fysieke netwerk-infrastructuur) en de psyche.

De unieke toegevoegde waarde is gekoppeld aan de virtuele laag van het digitale domein, waarin de nieuwe capaciteiten cyber-identiteiten en cyber-objecten besloten liggen. Deze onderdelen faciliteren de exploitatie van het cyber-domein. Hierna gaan we in op de concrete invulling van cyber-operaties.

Cyber-operaties

In onze inleiding definieerden we cyber-operaties als 'de inzet van cyber capabilities met het primaire (militaire) doel in of via cyberspace effecten te realiseren'.[59] Uiteindelijk dienen ook cyber-operaties een hoger (strategische bepaald) doel: het beïnvloeden van actoren in of via cyberspace.

Beïnvloeding 'in of via cyberspace' impliceert twee parallelle noties. Enerzijds worden effecten via cyberspace gerealiseerd. Cyberspace fungeert als vector voor een cyber-middel en biedt derhalve (ook) ruimte voor het gebruik van social media (zie hierna). Anderzijds worden effecten in cyberspace gerealiseerd: in de fysieke en/of de virtuele laag. Dit betreft bijvoorbeeld de inzet van software tegen luchtverdediging.

Cyber-operaties kunnen op zichzelf staan, of deel uitmaken van andere (kinetische) operaties.[60] Net als in Nederland beogen meerdere staten cyber-operaties te integreren in hun reguliere militaire operaties.[61] Dat laatste was bijvoorbeeld zichtbaar bij

57 NDD (2013)101.

58 Zie: P. Ducheine, J. Voetelink, J. Stinissen & T. Gill, 'Towards a Legal Framework for Military Cyber Operations', in: Ducheine, Osinga & Soeters (eds.), *Cyber Warfare: Critical Perspectives* (2012)101-128.

59 Schmitt (2013) *Tallinn manual*, 258: 'The employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace'.

60 T. Gill & P. Ducheine, 'Anticipatory Self-Defence in Cyber Warfare', in: M. Schmitt (Ed.), *Cyber War and International Law* (International Law Studies 2012, Newport: Naval War College Press) <www.usnwc.edu/Publications/International-Law-Studies-(1).aspx>.

61 Voor nationale militaire cyber -doctrines: E. Tikk (2011) *Frameworks for International Cyber Security, National Cyber Security Policies and Strategies*, via <www.ccdcoe.org/284.html>. Zie D. Cameron (2010), *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Rewiev* 27 (2010), via <www.official-documents.gov.uk/document/cm79/7948/7948.asp>: 'Future conflict will see cyber operations conducted in parallel with more conventional actions in the maritime, land and air environments'.

operatie *Orchard* in september 2007, waarbij (vermoedelijk) Israël een luchtaanval uitvoerde op een Syrische nucleaire installatie in Al-Kibar.[62] Daarbij is de Syrische luchtverdediging met een parallelle cyber-operatie (tijdelijk) gemanipuleerd.[63]

In de literatuur worden cyber-operaties vaak beschreven via een fasering waarin verschillende (deel)doelstellingen herkenbaar zijn.[64] Cyber-operaties kunnen – afhankelijk van de doelstelling – deze gehele fasering (zie figuur 8: operatie C) of slechts een deel daarvan omvatten. Afhankelijk van het beoogde effect zullen bepaalde cyber-capaciteiten in specifieke fases worden ingezet. Zo bestaat er een middel (i.c. software) om kwetsbaarheden in netwerken te 'scannen' zodat een toegang tot een systeem gevonden kan worden (zie figuur 8: operatie A). Andere software verzamelt – na intrusie – in een netwerk informatie (idem: operatie B). Anders gezegd: los van én binnen dit generieke model bestaat een diversiteit aan cyber-capaciteiten die voor verschillende (deel)doelstellingen zijn in te zetten.

In beginsel staat niets in de weg om cyber-operaties ook via de manoeuvrebenadering en de geïntegreerde benadering vorm te geven. Sterker nog, gelet op de immer toenemende digitale afhankelijkheid van mensen en organisaties ligt een digitaal 'aangrijpingspunt' voor de hand.[65]
Hoe deze operaties nu precies vorm krijgen, bezien we hierna door achtereenvolgens in te gaan op adressaat, effecten en middelen/methoden bij cyber-operaties.

Adressaat en effecten

Cyber-operaties richten zich – via een adressaat – op tegenstanders, medestanders en neutralen en wel op de cyber capabilities in het (militaire) vermogen van die actoren. Hiervoor benoemden we die capabilities: personen, objecten en psyche alsmede de virtuele afspiegelingen cyber-objecten en cyber-identiteiten.
Directe effecten van cyber-operaties liggen in de niet-fysieke dimensie door 'contact' in de virtuele laag met cyber-objects en cyber-identiteiten. Bijvoorbeeld omdat een cyber-object niet meer functioneert.

Cyber-operaties steunen daarnaast op indirecte, secundaire effecten - zowel in het fysieke als niet-fysieke vlak.[66] Mensen en objecten in de

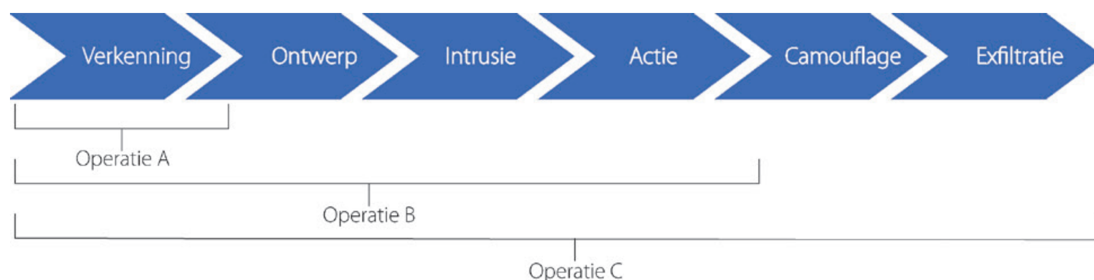
62 A. Garwood-Gowers, 'Israel's Airstrike on Syria's Al-Kibar Facility: a Test Case for the Doctrine of Pre-Emptive Self-Defence?', in: *Journal of Conflict & Security Law* 16 (2) 263-291: D. Gartenstein-Ross & J.D. Goodman (2009), 'The Attack on Syria's al-Kibar Nuclear Facility', in: *Focus Quarterly*, Spring, via <www.jewishpolicycenter.org/826/the-attack-on-syrias-al-kibar-nuclear-facility>; BBC News (Oct. 2, 2007), 'Israel admits air strike on Syria', via <news.bbc.co.uk/2/hi/middle_east/7024287.stm>.

63 D.A. Fulghum & D. Barrie (2007), 'Israel Used Electronic Attack in Air Strike Against Syrian Mystery Target', in: *Aviation Week* (8-10-2008) 28, via: <www.freerepublic.com/focus/f-news/1908050/posts>.

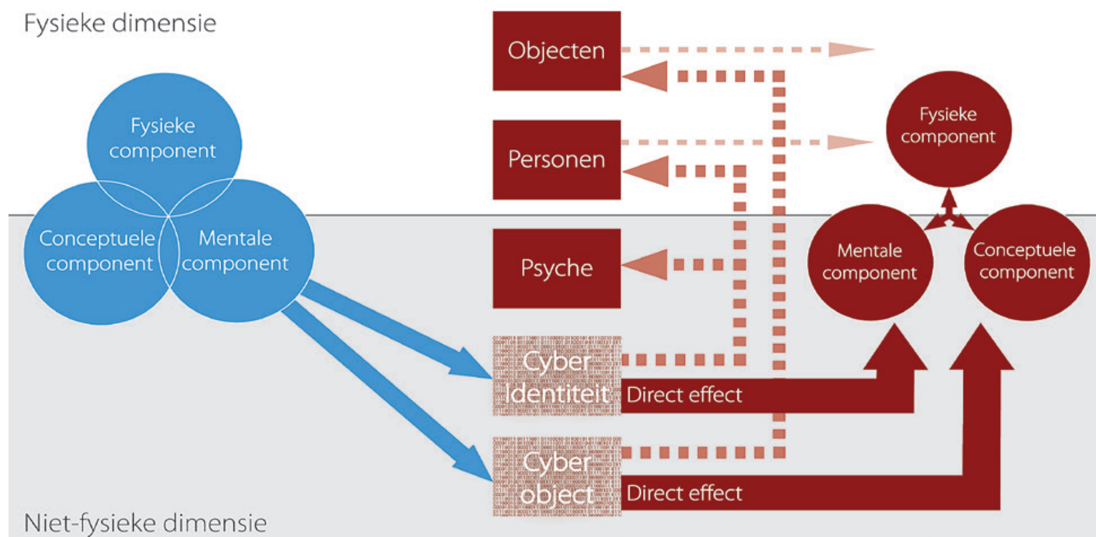
64 Zie: Andress & Winterfeld (2011)171: Reconnaisance, scan, access, escalate, exfiltrate, assault, sustain; Janczewski & Colarik (2008), Verkenning, binnendringen, uitbreiden, actie, bewijs verwijderen); Grant, Venter & Eloff (2007), *Footprinting, reconnaissance, vulnerability identification, penetration, control, embedding, data extraction or modification, attack relay, attack dissemination*.

65 Zie ook Qiao Liang and Wang Xiangsui, *Unrestricted Warfare*, Beijing: PLA Literature and Arts Publishing House, February 1999, via <m.tech.uh.edu/faculty/conklin/IS7033Web/7033/Week2/unrestricted.pdf>, 199: 'One hacker + one modem causes an enemy damage and losses almost equal to those of a war'.

66 W.A Owens, K.W. Dam, & H.S. Lin, *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities* (Washington D.C., National Academic Press, 2009) 127.



Figuur 8. Generieke fasering in cyber-operaties



Figuur 9. Adressaat in cyber-operaties

fysieke dimensie worden indirect beïnvloed door operaties tegen cyber-identiteiten en cyber-objecten. Dat geldt ook voor de samenhang. Door operaties tegen bijvoorbeeld cyber-objecten van communicatiesysteem kan een *common operational picture en situational awareness* van de tegenpartij verstoord of verdraaid worden, waardoor de samenhang in vermogen gedegradeerd wordt.

De psyche van mensen wordt indirect beïnvloed door cyber-objecten aan te grijpen en cyber-identiteiten te manipuleren. Bijvoorbeeld door mobiel internet te ontregelen en nepberichten aan bestaande accounts toe te voegen. We hebben deze (in)directe effecten in figuur 9 gevisualiseerd.

Middelen en effecten

Effecten van cyber-operaties treden zoals gezegd uiteindelijk op in de fysieke én niet-fysieke lagen van cyberspace. De beoogde effecten van (delen van) cyber-operaties wisselen naargelang de doelstelling. Het betreft een breed spectrum, variërend van het verbeteren van informatieposities tot disruptieve acties zoals Stuxnet.[67]

Ter illustratie van dit spectrum – en zonder compleet te willen zijn[68] – beschrijven we middelen en methoden die tegen cyber-identiteiten en cyber-objecten kunnen worden ingezet. De mate van detaillering wijkt af van het voorgaande deel: dat heeft als doel deze relatief onbekende materie met voorbeelden te illustreren.

Waar nodig maken we onderscheid tussen tegenstanders, medestanders en neutralen: de beoogde effecten houden verband met de aard van deze drie groepen. Anders gezegd: bij medestanders zullen vaak constructieve effecten beoogd zijn; bij tegenstanders disruptieve.

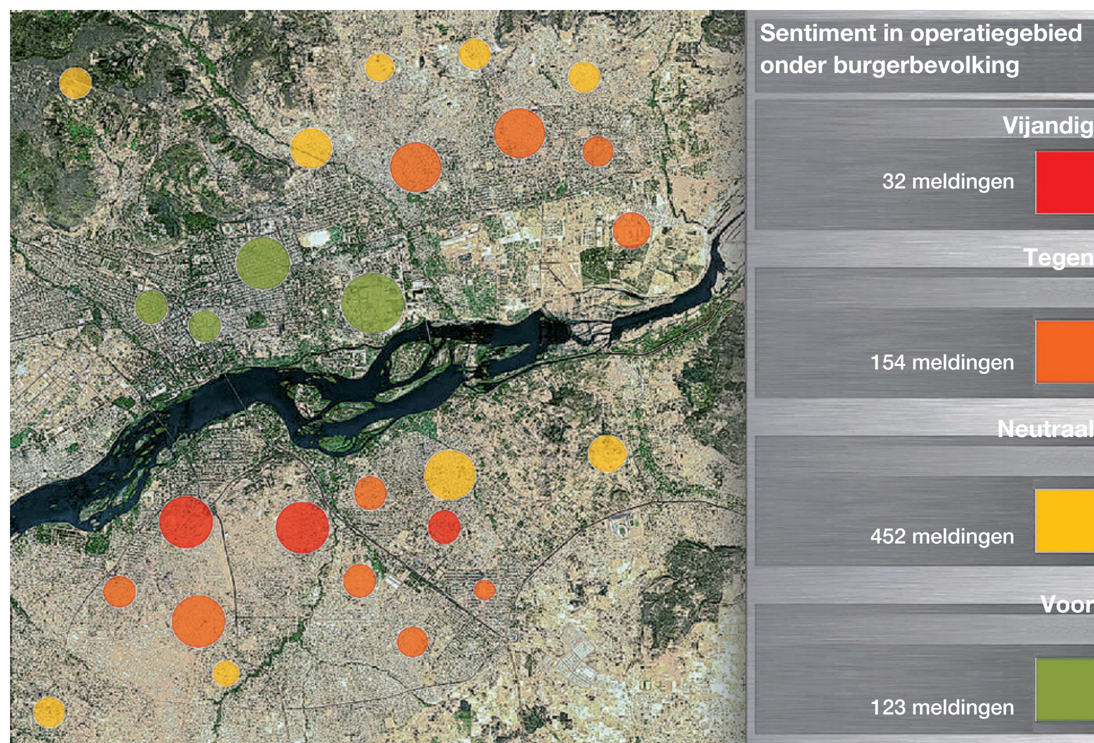
Exploitatie van cyber-identiteiten

Het feit dat een groot deel van de samenleving – individuen en groepen – een cyber-identiteit heeft, deze (actief) gebruikt en daar steeds afhankelijker van wordt,[69] maakt het interessant over capaciteit(en) te beschikken om deze te exploiteren.

67 Zie o.a. H.S. Lin, 'Offensive Cyber Operations and the Use of Force', in: *Journal of National Security Law & Policy*, 4 (2010) 63-85; T. Rid & P. McBurney (2012) 'Cyber-Weapons', in: *The RUSI Journal* 157(1) 6-13. Tabansky (2011).

68 Technologische ontwikkeling en voorstellingsvermogen begrenzen de potentiële mogelijkheden en middelen.

69 Zie het voorbeeld van het betalingsverkeer uit de inleiding. Zie ook F. Osinga, 'Introducing Cyber Warfare', in: Ducheine, Osinga & Soeters (eds.) *Cyber Warfare – Critical Perspectieves* (2012)1-18.



Figuur 10. Datamining

Exploitatie kan bestaan uit het verzamelen van informatie (a), het verspreiden van informatie (b) en/of het impliciet of expliciet beïnvloeden van personen – medestanders, tegenstanders of neutralen – zowel thuis of in een operatiegebied (c). Indien cyber-identiteiten digitaal toegankelijk zijn kunnen deze ook gemanipuleerd of vernietigd worden (d).

- *Informatie verzamelen*

Cyber-identiteiten kunnen worden benaderd om informatie te verzamelen, waardoor een beeld kan worden gegenereerd van het sentiment van individuen, van groepen en de samenleving. De informatie over cyber-identiteiten bevindt zich in open bronnen (*social-networking sites*, blogs en dergelijke) en in niet-openbare bronnen (mailverkeer e.d.).

Informatie verzamelen over één individu is niet arbeidsintensief; over een samenleving of operatiegebied daarentegen wel. De hoeveelheid beschikbare data maakt het lastig de 'juiste' informatie te vinden. Ter illustratie: per minuut worden 684.478 Facebook-berichten gedeeld, 100.000 Tweets gepost, 3.600 *Instagram*-foto's geplaatst, 347 nieuw *Wordpress*-blogs aangemaakt en 48 uur video via *YouTube* geüpload.[70]
Om uit deze overvloed relevante informatie te kunnen destilleren, is software ontwikkeld die het sorteren, aggregeren, correleren, clusteren en *geo-taggen* van open informatie ondersteunt.[71] Met deze *datamining tool*' kan een beeld gegenereerd worden van het sentiment in het thuisland of operatiegebied via de cyber-identiteiten (zie figuur 10).[72]

Om niet-openbaar informatie van cyber-identiteiten te verkrijgen zijn andere, meer invasieve methoden nodig. Bijvoorbeeld door dataverbindingen af te luisteren of af te tappen,

70 N. Spencer (2012) 'How Much Data is Created Every Minute?' via: <visualnews.com/2012/06/19/how-much-data-created-every-minute/>.
71 Pfleeger & Pfleeger (2007) 367.
72 Ter illustratie van de werking in thuisland: <nederlandsespoorwegen.crowdmap.com>.



Figuur 11. Tweet op zoek naar draagvlak en geld

door gebruikers te verleiden c.q. te misleiden tot het afgeven van toegangsgegevens: *social engineering* genaamd. Of door in te breken (hacken) in accounts.[73] Bij één persoon is de benodigde tijd te overzien; een (bevolkings-) groep 'handmatig' afluisteren is zeer arbeidsintensief.

Inlog- en accountgegevens zouden op grote(re) schaal kunnen worden achterhaald door twee vormen van social engineering: *phishing* of *pharming*.[74] De doelgroep krijgt bijvoorbeeld een legitiem ogend bericht waarin een gebruiker gevraagd wordt in te loggen op een clandestiene website (*pharming*) of een bijlage te openen, waardoor diens computersysteem gecompromitteerd wordt (*phishing*).[75] De inloggegevens die dit zou opleveren zouden op grote schaal te exploiteren zijn met datamining tools.[76]

De informatiepotentie van cyber-identiteiten binnen open en niet-openbare bronnen is enorm en versterkt langs digitale weg de inlichtingencapaciteit (thuis en in operatiegebieden).

● *'Soft cyber': passieve inzet van cyber-identiteiten*

Via social media en internet kunnen cyber-identiteiten (van medestanders, neutralen en zelfs tegenstanders) passief worden benaderd met als doel informatie te verspreiden of een dialoog te voeren. Dit loopt via eigen cyber-identiteiten: via accounts die gelieerd zijn aan de overheid, krijgsmacht, politici of militairen.[77] Zie de profielen en accounts van de minister (zie figuur 6) en krijgsmacht (onder-)delen op bijvoorbeeld Facebook, Linkedin en Hyves, foto- en videohosting internetservices (zoals YouTube en Flickr),[78] Wikipedia-pagina's[79] en blogs (bijvoorbeeld *Tumblr* en *Wordpress*).[80]

Het beoogde effect is bijvoorbeeld het vergroten van het draagvlak voor de krijgsmacht en haar missies, wat de eigen mentale component ten goede komt.[81] Een illustratie is de tweet van Peter van Maurik, *geretweet* door KTZ Rob Hunnego, samen goed voor duizend volgers (zie figuur 11).

Dit typeren we als een vorm van 'soft cyber': het effect is niet-fysiek, de operatie loopt via cyberspace met internet als vector.
De inzetmiddelen (eigen cyber-capaciteit) én het adressaat zijn cyber-identiteiten, waarmee indirect mensen beïnvloed kunnen worden. 'Soft cyber' is daarmee ook een specifiek middel in informatieoperaties.

● *'Soft cyber' in operatiegebieden*

Passieve soft cyber wordt ook in operatiegebieden toegepast.[82] De werking is vergelijk-

73 Pfleeger & Pfleeger (2007) 404-414.
74 Andress & Winterfeld (2011) 140-141.
75 Andress & Winterfeld (2011) 140-141.
76 Andress & Winterfeld (2011) 144.
77 Zie ook <defensie.nl/actueel/social_media>.
78 Youtube.com/user/defensie.
79 Wikipedia.org/wiki/Koninklijke_Landmacht.
80 US DoD, Directive-Type Memorandum (DTM) 09-026 (2010, Feb) *Responsible and Effective Use of Internet-based Capabilities*,5 , via: www.carlisle.army.mil/DIME/documents/DODNewMediaPolicyFeb10.pdf.
81 Zie de oproep 'soft cyber': 'Cyber en militair vermogen', in: *Militaire Spectator* 181 ((2012) (12).
82 Zie: J. van der Meulen & R. Moelker, 'Digital Duels in the Global Public Sphere. Social Media in Civil Society and Military Operations', in: Ducheine, Osinga & Soeters (2012). *Cyber warfare: critical perspectives*, 141.

baar met hetgeen hiervoor is beschreven, maar dan gericht op tegenstanders, medestanders of neutralen in het buitenland. Bekende voorbeelden zijn de 'verbale' twitterduels uit de Tweede Gazaoorlog tussen *@IDFSpokesperson* (216.112 volgers) en Hamas. Volgers van de *@IDFSpokesperson* en Facebook-vrienden ontvangen deze afbeelding (zie figuur 12)[83].
Nederlands zet vooralsnog slechts beperkt cyber-identiteiten in uitzendgebieden in en concentreert zich daarbij op het thuisfront.[84] Voor zover 'operationele veiligheid' of OPSEC een reden voor terughoudendheid is,[85] kan deze geborgd worden door gebruikers goed te instrueren.[86] Indien (nog steeds) wordt gedacht dat de bevolking in potentiële operatiegebieden geen toegang heeft tot social media of andere media, wordt dit door huidige ontwikkelingen tegengesproken.

Vooral in het Midden-Oosten (2640 procent toename tussen 2000-2012), Afrika (3607 procent)[87] en Azië (860 procent) groeit mobiel internet sterk.[88] De rol van social media in de Arabische Lente is een mooi voorbeeld van deze ontwikkeling.[89]
De inzet van cyber-identiteiten tijdens operaties kan samenvallen met (het doel van andere) informatieoperaties, *Strategic Communication* en bijvoorbeeld *key leader engagement*.
Het lijkt een veelbelovende maar relatief onontgonnen capaciteit. Key leader engagement kan ook langs deze digitale weg vorm krijgen (zie hierna).

● *Actieve beïnvloeding van cyber-identiteiten*
Cyber-identiteiten kunnen (ook) gericht en actief worden benaderd om indirect andere personen of groepen te beïnvloeden. Op basis van bijvoorbeeld sentiment of achtergrond, te achterhalen met datamining tools, en met herleide gebruikersgegevens (cyber-identiteiten) is interactie met individuen of groepen mogelijk.

Persoonlijke interactie is daarbij effectiever dan generieke communicatie, maar uiteraard ook arbeidsintensiever. Efficiënter én effectiever is het aanspreken van sleutelfiguren die ook weer via datamining bepaald kunnen worden.[90] Deze werkwijze heeft overeenkomsten met



Figuur 12. IDF-bericht
(Tweet van @IDFSpokesman en IDFBlog.com)

key-leader engagement binnen klassieke informatieoperaties.[91]
Een bijzondere vorm van disruptieve beïnvloeding is het toebrengen van imagoschade aan key leaders. De geloofwaardigheid of reputatie van vooraanstaande personen kan via cyber-identiteiten op effectieve wijze worden aangetast, met eventuele 'uitschakeling' van de persoon als gevolg.

83 Tweet @IDFSpokesman (en IDFBlog.com) tijdens Tweede Gazaoorlog (Operatie *Pillars of Defence*), via: <www.idfblog.com/wp-content/uploads/2012/11/checklistinfographic.jpg>.
84 Zie: <defensie.nl/missies/actueel/algemeen/2013/03/12/46203777/Weekoverzicht_Defensie_operaties_video>.
85 Voor overwegingen omtrent OPSEC zie: K.C. Dreijer (2010) *Social Media: Friendly Fire op het Internet?* Bachelorscriptie NLDA, via: <defbib.kma.nl/art2/pdf/ada/Dreijer%20K.C.pdf>.
86 Zie ook *US Army Social Media Handbook* (2012), Optimizing Online Engagement, 2 , via: < armylive.dodlive.mil/index.php/2011/01/u-s-army-social-media-handbook-is-here/>.
87 Zie *NRC Handelsblad*,18 juni 2013, Afrika springt het digitale tijdperk in.
88 *Internet Usage Statistics: The Internet Big Picture*, via: <internetworldstats.com/stats.htm>.
89 Zie: <syriatracker.crowdmap.com>.
90 Zie: <newsroom.edelmanpr.nl/jeanine-hennis-plasschaert-meest-invloedrijke-kabinets-lid-op-twitter/>.
91 LDP I,140. Zie: M. Kitzen, S. Rietjens, F. Osinga, 'Learning soft power the hard way, military adaptation by the Netherlands' Task Force Uruzgan, in: T. Farrell, F. Osinga & J. Russell (Eds.), *Military Adaptation in Afghanistan* (Stanford University Press, 2013).

- *Cyber-identiteiten manipuleren of vernietigen*

Indien cyber-identiteiten toegankelijk zijn, bijvoorbeeld doordat een wachtwoord via social engineering verkregen is, kan het gemanipuleerd, gemuteerd, ontoegankelijk gemaakt of vernietigd worden.

Exploitatie van cyber-objecten

Steeds meer (en steeds vaker) worden fysieke objecten op internet aangesloten om snelle informatieoverdracht te faciliteren en gebruikersgemak te vergroten.[92] Voorbeelden zijn: auto's, printers, huishoudelijke elektronica en zelfs pacemakers en insulinepompen.[93] Deze fysieke objecten hebben een digitale representatie in het cyber-domein, het cyber-object.
Analoog aan het beïnvloeden van fysieke personen (en hun psyche) via cyber-identiteiten, kunnen fysieke objecten worden gemanipuleerd via hun virtuele afspiegeling: cyber-objecten. Deze optie is bij uitstek geschikt om het digitale vermogen van de krijgsmacht te vergroten.

- *Inzet fysieke objecten*

Een cyber-operatie zou kunnen bestaan uit het aanbieden van infrastructuur. Bijvoorbeeld in de vorm van een internetcafé, (mobiele) gsm-mast, routers, servers, (WIFI-)netwerk. Op deze manier kan informatie worden verzameld over de gebruikers van deze fysieke (en digitale) objecten.[94] Zo zou ook een internetserviceprovider kunnen worden opgericht, of een IT-beveiligingsbedrijf waarmee cyber-objecten en cyber-identiteiten (van klanten) benaderbaar worden.

- *Monitoren cyber-objecten*

Via (eigen) cyber-identiteiten kan online informatie worden verzameld over een aan te grijpen of te beïnvloeden cyber-object. Dit kan ongemerkt en zonder direct contact te maken met het cyber-object via open bronnen zoals databases (e.g. *Shodan HQ*),[95] handleidingen en websites met informatie over het cyber-object.

Een alternatief is het actief monitoren met specifieke software (een eigen cyber-object) die het cyber-object in kaart brengt. Deze software (bijvoorbeeld *Nmap* of *Metagoofil*)[96] verzamelt informatie over de zwakheden, architectuur, locatie en een variëteit aan andere bruikbare informatie.[97] Deze informatie kan inzicht bieden over het functioneren, beheer, locatie en kwetsbaarheden van het cyber-object en het gekoppelde fysieke object.

- *Externe manipulatie cyber-objecten*

Cyber-objecten kunnen ook worden gemanipuleerd. De meest basale vorm is van buitenaf, zonder toegang te forceren. Met een zogeheten (*distributed*) *denial of service* of (D)DOS-aanval wordt het cyber-object, bijvoorbeeld een digitale dienst als DigiD, overladen met dataverkeer waardoor deze tijdelijk onbereikbaar is.[98]
Om een (D)DOS aanval uit te kunnen voeren is een eigen (of overgenomen) bot-netwerk[99] nodig[100] of worden sympathisanten gemobiliseerd.[101] Daarnaast bestaan ettelijke methoden om cyber-objecten te manipuleren.[102] De technische beschrijving van de modus operandi van dit soort aanvallen valt te ver buiten de doelstelling van deze bijdrage.

92 Ook wel het '*Web of objects*' of '*the Internet of Things*' genaamd.

93 Daily Mail online (10 april 2012), *Hackers 'can gain access to medical implants and endanger patients' lives'*. <http://www.dailymail.co.uk/health/article-2127568/Hackers-gain-access-medical-implants-endanger-patients-lives.html>.

94 Zoals ten tijde van de G20-top in London (2009), zie *NRC Handelsblad*, 17 juni 2013, *Britse geheime dienst luisterde G20 in Londen af*.

95 *Shodan* is een zoekmachine die een gebruiker in staat stelt om specifieke systemen en computers te vinden en bekende data te raadplegen aangaande het systeem, in tegenstelling tot de Google zoekmachine die informatie vindt.

96 *Nmap* stelt gebruikers in staat om cyber-objecten te scannen op – onder meere – open (toegangs-)poorten, kwetsbaarheden en besturingssysteem. *Metagoofil* zoekt naar metadata (data met gegevens over data). Uit deze metadata kan bijvoorbeeld worden opgemaakt wie de data heeft aangemaakt en aangepast; waar de data opgeslagen is geweest; welke wijzigingen in tekst of data er zijn gemaakt, de locatie waar een foto is gemaakt en met welk toestel, e.d..

97 Andress & Winterfeld (2011) 88-100.

98 Zoals onlangs (waarschijnlijk) het geval was bij DigiD en iDeal: zie NCSC, 9-4-2013, *DDOS-aanval zorgde voor verstoring bereikbaarheid websites*, zie: <www.ncsc.nl/actueel/nieuwsberichten/ddos-aanval-zorgde-voor-verstoring-bereikbaarheid-websites.html>.

99 Een bot-netwerk bestaat uit gekoppelde gecompromitteerde (gehackte) systemen die ter beschikking staan van een cyber-operator om te gebruiken in een variëteit aan cyber-operaties, waaronder een DDOS.

100 Zie NCSC, 15-5-2013, *Factsheet Continuiteit van online diensten*, <www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets>.

101 Zoals Anonymous dit toepast. Zie <resources.infosecinstitute.com/loic-dos-attacking-tool>.

102 Bijvoorbeeld via *domain name servers* (DNS), routers en lokale *host* files: Pfleeger & Pfleeger (2007) 422, 429-432. Ook door inbedding in hardware, operating systems, veranderingen in programmatuur en de updates daarvan, *spoofing* van IMEI- en MAC-adressen, e.d.

● *Intrusie voor interne manipulatie*

Cyber-objecten zijn van binnenuit beter te manipuleren, hetgeen toegang vereist.[103] Intrusie valt op diverse manieren te realiseren. Eenvoudige wachtwoorden kunnen worden gekraakt met software als *Hydra* en *John the Ripper*,[104] of via social engineering (phishing of pharming) en eerder gecompromitteerde wachtwoord-databases[105] herleid worden.[106]

Toegang kan ook worden gerealiseerd door (bekende en onbekende) kwetsbaarheden (de zogeheten *exploits*) van een cyber-object te benutten. Bekende exploits van veelgebruikte besturingssystemen en databases zijn online beschikbaar.[107] Bovendien bestaat er software zoals *Metasploit en Immunity CANVAS*[108] om deze exploits effectief te benutten.[109] Sommige bedrijven specialiseren zich in nog onbekende kwetsbaarheden (*zero-days*) en verkopen deze aan de hoogste bieder.[110]

Na intrusie kan de toegang tot het cyber-object worden bestendigd en uitgebreid door bepaalde *payloads* uit te voeren op het systeem.[111] Denk aan het openen van een digitale poort van het fysieke of cyber-object,[112] het installeren van een (*reverse*) *shell*,[113] toevoegen van geautoriseerde gebruikers (bijvoorbeeld administrators) en het creëren van *backdoors*.[114] Zo ontstaan meer mogelijkheden (bevoegdheden en bewegingsruimte) binnen het cyber-object en wordt toekomstige toegang gewaarborgd. Op deze manier kunnen ook de intrusie, actie en manipulatie worden 'gecamoufleerd' (zie figuur 8).

● *Interne manipulatie*

Vervolgens kan het cyber-object door de indringer worden gemanipuleerd. Manipulatie kan onder meer bestaan uit het veranderen van de instellingen, het beheer, het functioneren en het gebruik van het cyber-object (en het gekoppelde fysieke object). Het cyber-object wordt dan door anderen gecontroleerd en beheerst.

Zo kunnen ondersteuningssystemen voor commandovoering worden verstoord, kan desinformatie worden verspreid, toegang worden ontzegd, informatie worden gemuteerd of onttrokken.[115]

Indien het cyber-object is gekoppeld aan een computer kan deze als extra computervermogen voor basale taken worden ingezet. Bijvoorbeeld het verspreiden van berichten (*spam*) en software, het kraken van wachtwoorden of voor (D)DOS aanvallen. Daarnaast is de gecompromitteerde computer beschikbaar als aanvalsvector bij toekomstige cyber-operaties. Zodoende zijn cyber-aanvallen te lanceren vanaf de gecompromitteerde computer en niet vanaf eigen systemen, hetgeen misleiding en verrassing ten goede komt en de herkomst camoufleert.

Indien het overgenomen cyber-object een besturingssysteem van fysieke objecten betreft, kunnen deze fysieke objecten worden gemanipuleerd. De inzet van Stuxnet tegen het

103 Via het besturingssysteem of de database van het doel. In het geval van SQL injectie (SQLi) is het discutabel of toegang tot een systeem daadwerkelijk een premisse is om een systeem te manipuleren.

104 *Hydra* kan worden gebruikt om een groot aantal veelgebruikte of waarschijnlijke wachtwoorden en gebruikersnamen uit te proberen. *John the Ripper* kan worden gebruikt om wachtwoord *hashes* (versleutelde wachtwoorden) in te voeren en uit te proberen.

105 Zie: <pastebin.com/XvbzgW64>.

106 Andress & Winterfeld (2011) 100-101.

107 Zie bijvoorbeeld voor Windows XP: <www.exploit-db.com/platform/?p=windows>.

108 *Metasploit* kan gebruikt worden om (1) systemen te scannen, (2) een *exploit* te selecteren voor het gescande systeem, (3) deze te voorzien van een *payload* en (4) de *exploit* met *payload* uit te voeren op het doelsysteem. *Immunity CANVAS* kan worden gebruikt om (semi-)automatisch toegang te krijgen tot doelsystemen en deze vervolgens te exploiteren via een scala aan *exploits* en *payloads*.

109 Andress & Winterfeld (2011)103-105.

110 Het Franse Vupen is een bedrijf dat *zero-days* verkoopt aan voornamelijk overheden en bedrijven: A. Greenberg, in: *Forbes.com* (23 maart 2012), 'Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits', via <forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>; J.M. Schwartz, *Blackhole Botnet Creator Buys up Zero Day Exploits*, in: <www.informationweek.com/security/vulnerabilities/blackhole-botnet-creator-buys-up-zero-da/240145769>.

111 Andress & Winterfeld (2011) 109.

112 Computers, netwerken en andere systemen maken gebruik van 'poorten' om onderling te communiceren. Zo kan een poort dicht zijn of gebruikt worden om te luisteren of zenden. Poort 80 op een pc wordt (standaard) bijvoorbeeld gebruikt voor *Hypertext Transfer Protocol* (http), oftewel het surfen op het internet.

113 *Reverse shells* zorgen ervoor dat een doel-systeem verbinding zoekt met het systeem van de hacker. *Shells* in het algemeen zorgen ervoor dat de *operator* bepaalde opdrachten kan in- en uitvoeren op het doel-systeem.

114 *Backdoors* zorgen ervoor dat een hacker een alternatieve toegang heeft tot het systeem, die niet geblokkeerd wordt door beveiligingsupdates in software.

115 *Deception, disruption, denial, degradation, & destruction* (5 D's), in de duiding van Andress & Winterfeld, (2011) 110.

Adressaat	*Cyber-identiteit*	*Cyber-object*
Effect		
Constructief	Info verzamelen • Datamining • Social engineering (o.a. Phishing, Pharming) Info verspreiden • Passieve soft-cyber Interactie Beïnvloeden • Actieve soft-cyber, o.a. key leader engagement	Scannen Info verzamelen Exploits ontwerpen tbv intrusie
Disruptief	Beïnvloeden / misleiden Irrelevant maken Manipulatie Blokkeren Vernietigen	Extern manipuleren • Kraken • Overbelasten Intrusie Intern Manipuleren • Camoufleren • Upgraden • Disfunctioneren • Misbruiken (bot of vector) • Blokkeren Vernietiging

Tabel 1: Cyber-activiteiten

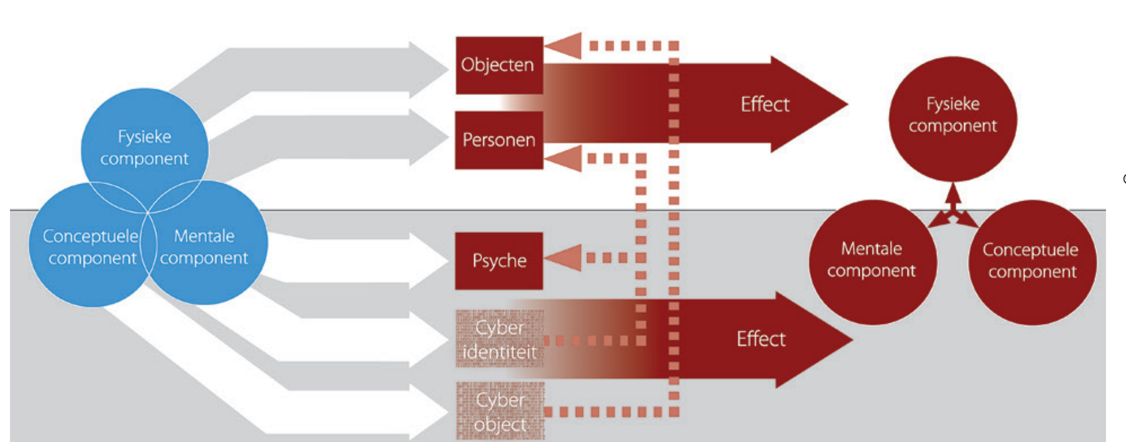
Iraanse atoomprogramma door het aanpassen van de besturing van de centrifuges voor uraniumverrijking is hier een voorbeeld van.[116]

• *Vernietigen cyber-objecten (offensieve actie)*
Na manipulatie functioneert het cyber-object nog wel, maar op een andere manier. Vernietiging leidt tot disfunctioneren van het cyber-object, bijvoorbeeld door het wissen van data of besturingssystemen. Vernietiging is alleen compleet indien er geen back-up beschikbaar is. Met een *back-up* zal 'slechts' sprake zijn van een tijdelijke onderbreking van de functionaliteit van het cyber-object.[117]

Toegang tot het cyber-object en beheerprivileges zijn een vereiste voor digitale vernietiging (i.e. wissen); deze kunnen via de eerder genoemde methoden worden gerealiseerd.

Effecten
Cyber-operaties zijn volgens de NDD een variant van informatieoperaties.[118] Deze laatste beogen niet-fysieke effecten: het beïnvloeden van tegenstanders, medestanders en neutralen. Met cyber-operaties kunnen volgens onze analyse zowel (directe en indirecte) niet-fysieke als indirecte fysieke effecten worden bereikt.[119] De effecten van cyber-operaties worden primair bepaald door de (deel)doelstelling (zie figuur 8) van die operatie. In een verkennende fase is het beoogde effect 'beperkter' dan in de actie-fase, waarin een vergaand effect, bijvoorbeeld tijdelijke of permanente onbereikbaarheid, controle of zelfs destructie beoogd kan zijn. De effecten variëren van constructief tot disruptief.

116 D. Sanger, *Confront & Conceal: Obama's Secret Wars and Surprising Use of American Power* (Crown, New York, 2012).
117 *Wiper malware*, ontdekt op Iraanse systemen, is specifiek ontworpen is om snel data te vernietigen. Zie K. Zetter, K. (28 mei 2012), *Meet 'Flame', The Massive Spy Malware Infiltrating Iranian Computers*, via <wired.com/threatlevel/2012/05/flame/>.
118 NDD (2013) 99.
119 Zoals bijvoorbeeld Stuxnet.



Figuur 13. Militair vermogen en (cyber-)operaties

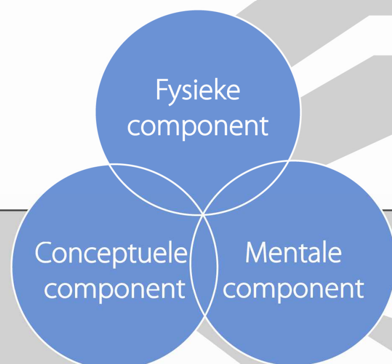
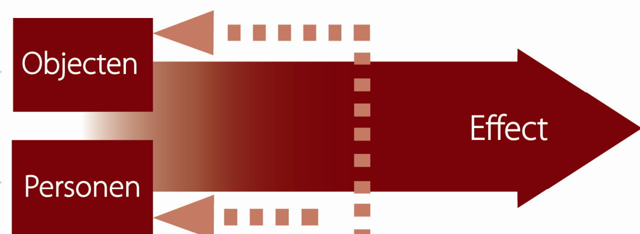
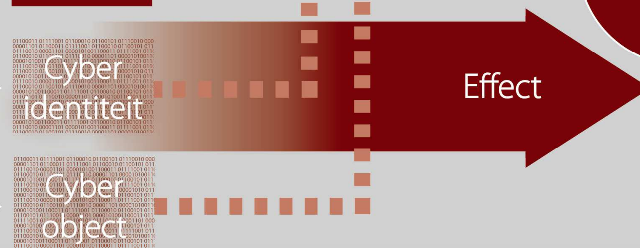
De effecten hangen uiteraard ook samen met het adressaat van de operatie. Manipulatie van cyber-objecten kan directe disruptieve gevolgen voor het cyber-object hebben, maar ook indirecte fysieke gevolgen voor het gekoppelde fysieke object. Manipulatie van cyber-identiteiten zal minder snel fysieke consequenties hebben. Maar gemanipuleerde cyber-identiteiten kunnen imagoschade creëren, waarmee personen 'irrelevant' te maken zijn. Uiteraard worden de effecten ook bepaald door de doelgroepen: tegenstanders, medestanders en neutralen. Disruptieve effecten bij medestanders zijn moeilijk voorstelbaar.
Het spreekt voor zich dat deze in cyber te realiseren effecten moeten bijdragen aan de politiek-strategische doelstelling waarvoor militair vermogen wordt ingezet. Met andere woorden, de ultieme effecten zullen moeten bijdragen aan strategisch te realiseren effecten waarvoor de krijgsmacht wordt ingezet.

Conclusie

Onze doelstelling was de plaats van cyber-operaties binnen militair vermogen te bepalen en te bezien hoe de krijgsmacht cyber-operaties (en cyber warfare) doctrinair kan operationaliseren. Uit onze analyse blijkt dat cyber-operaties – via een interpretatie van de niet-fysieke elementen – in gangbare modellen van militair vermogen passen. Ze zijn instrumenteel in het realiseren van strategische doelstellingen door het beïnvloeden van (het vermogen van) andere actoren. Cyber-operaties vinden plaats in of via het digitale domein, bestaande uit een fysieke en een niet-fysieke dimensie. De niet-fysieke dimensie van cyberspace, de virtuele laag (logical layer), maakt cyber-operaties bijzonder ten opzicht van operaties in het fysieke domein (en een aantal andere informatieoperaties). Deze virtuele laag bevat unieke capaciteiten, cyber-identiteiten en cyber-objecen, die om te zetten zijn in capabilities en daardoor bijdragen aan het totale eigen (militaire) vermogen. Cyber-operaties genereren effecten door zich te richten op de cyber-capaciteiten en capabilities in het (militaire) vermogen van andere actoren. Het adressaat van cyber-operaties bestaat uit de cyber-identiteiten en cyber-objecten in dat vermogen van anderen. De effecten zelf variëren van constructief tot disruptief en zijn veelal indirect ten opzichte van adressaten in de fysieke dimensie.

Twee misverstanden willen we aanstippen. Cyber warfare is meer dan 'het aanvallen van een hacker' of het 'targeten van een server', zoals regelmatig wordt gehoord. Een ander is de relatie tussen cyber-operaties en informatie-operaties. Cyber-operaties volgen qua principe informatieoperaties, maar qua adressaat nemen ze een unieke positie in. Ook 'soft cyber' operaties zijn daardoor afwijkend ten opzicht van gangbare informatieoperaties.

We willen verder volstaan met een integraal schema waarin de verschillende onderdelen van cyber een plaats krijgen binnen militair vermogen en dat bovendien een model voor cyber-operaties naast reguliere operaties in de andere domeinen representeert. Voor de overzichtelijkheid hebben we de doelgroepen medestanders en neutralen in dit schema niet gedetailleerd opgenomen. ■




Fysieke dimensie
Fysieke component
Conceptuele component
Mentale component
Objecten
Personen
Psyche
Cyber identiteit
Cyber object
Effect
Effect
Fysieke component
Mentale component
Conceptuele component
Niet-fysieke dimensie